Copyright © 2004 Global Technology Associates, Inc.

A Balanced Key Management

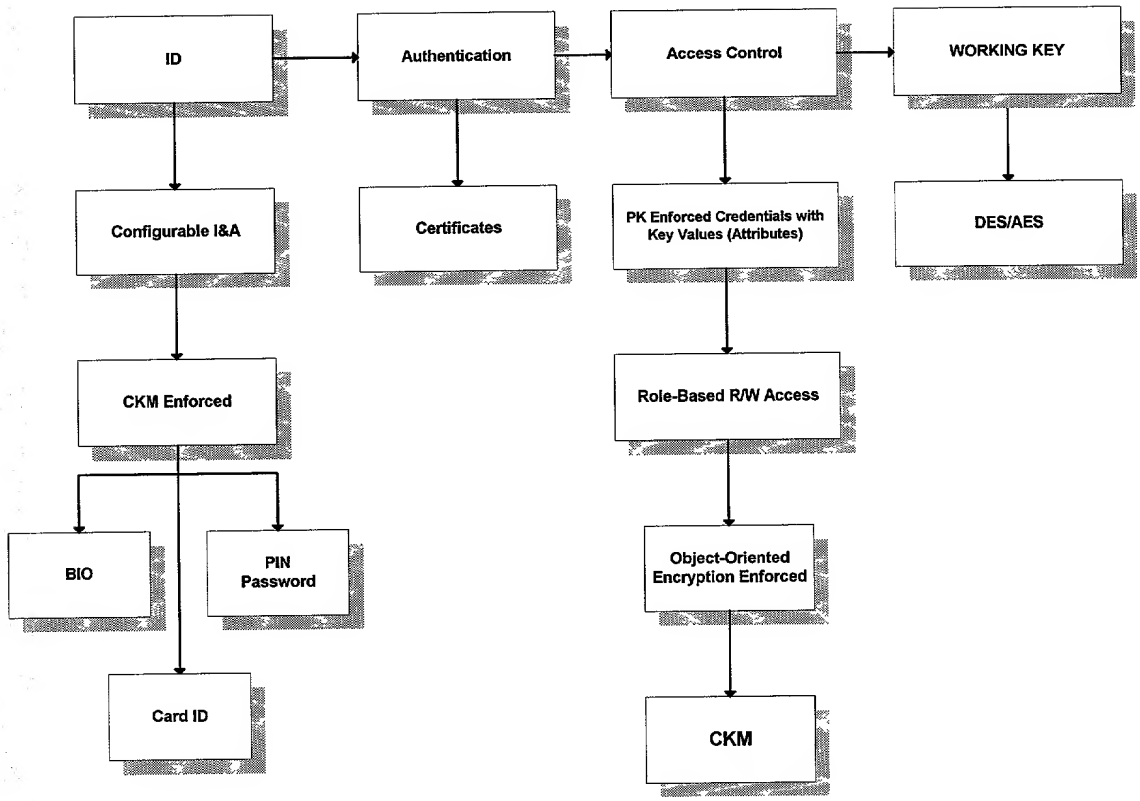


FIG. 1

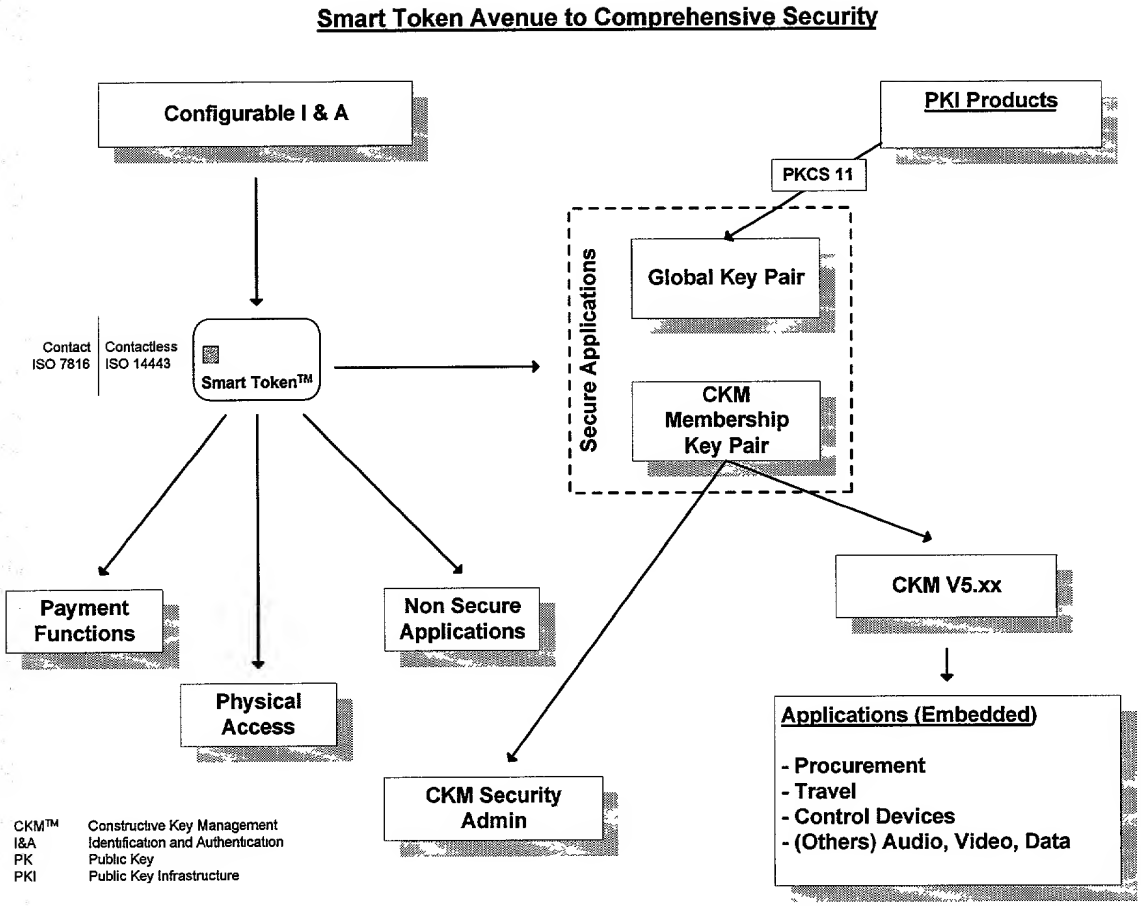
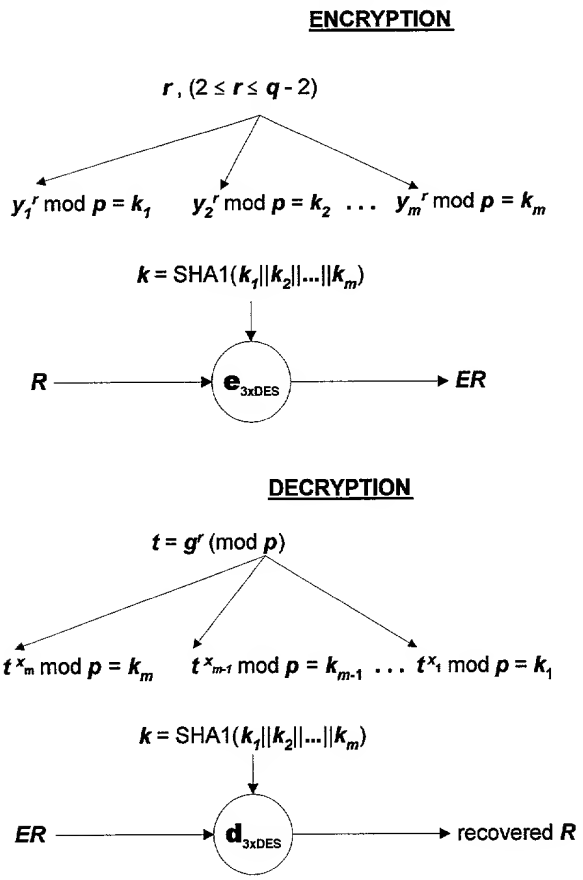

Smart Token Avenue to Comprehensive Security
Configurable I & A
PKI Products
PKCS 11
Secure Applications
Global Key Pair
CKM Membership Key Pair
Contact ISO 7816
Contactless ISO 14443
Smart Token™
Payment Functions
Physical Access
Non Secure Applications
CKM V5.xx
Applications (Embedded)
- Procurement
- Travel
- Control Devices
- (Others) Audio, Video, Data
CKM Security Admin
CKM™ Constructive Key Management
I&A Identification and Authentication
PK Public Key
PKI Public Key Infrastructure

FIG. 2

Diffie-Hellman Random Value Encryption and Decryption



Legend:

p	Diffie-Hellman prime modulus
q	Diffie-Hellman 160-bit prime
g	generator of group Z_p
m	number of labels
k_i	i^{th} derived key
k	two-key 3xDES key
r	Ephemeral Private Key
R	Random Value
ER	Encrypted Random Value
t	Ephemeral Public Key

FIG. 3

ANSI X9.69 Combiner Function

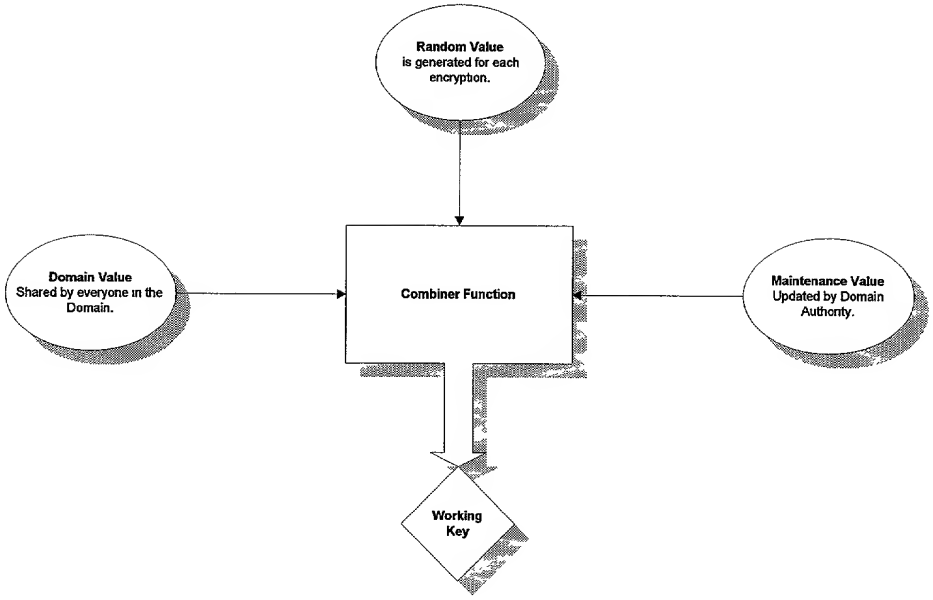
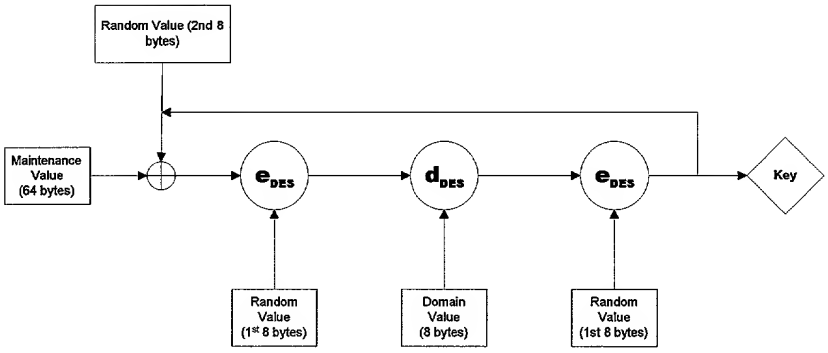


FIG. 4

ANSI X9.69 Combiner Function Using X9.52 (Triple DES CBC Mode)



Legend

e_{DES} DES encryption
d_{DES} DES decryption
$\oplus$ Exclusive-OR

FIG. 5

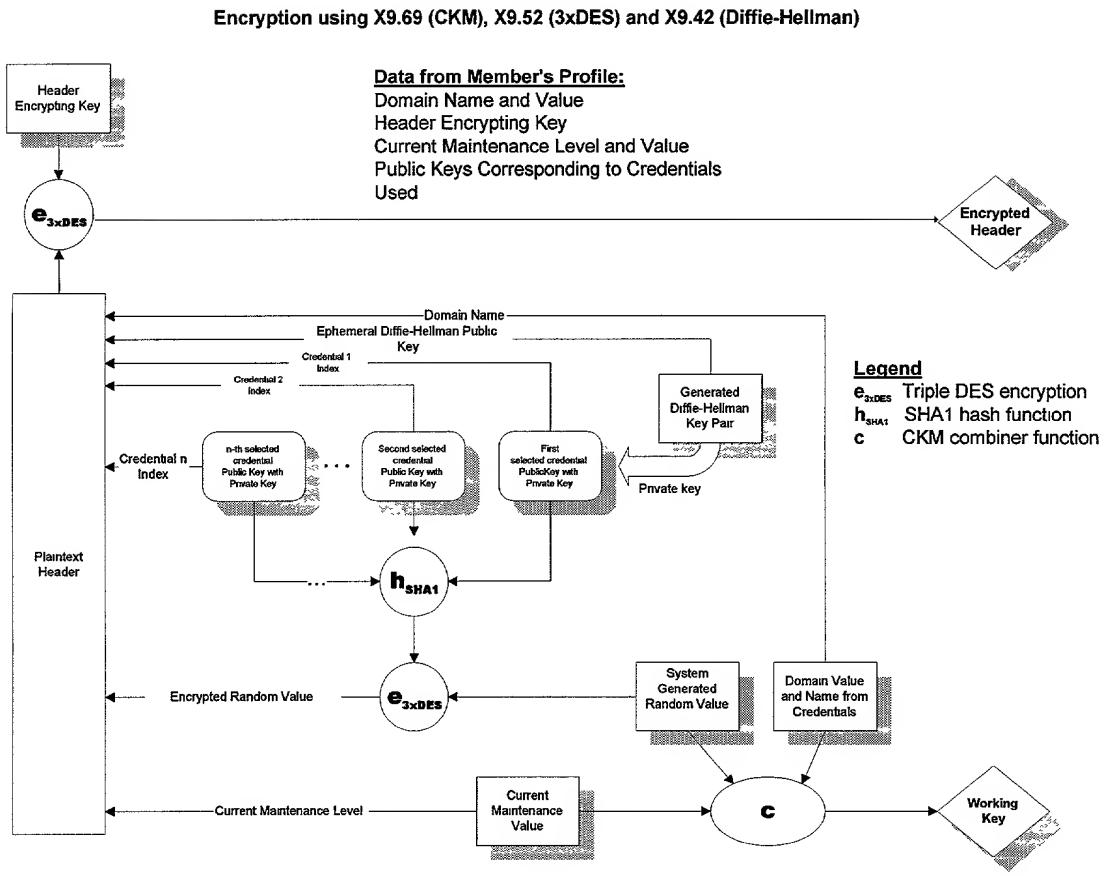

Encryption using X9.69 (CKM), X9.52 (3xDES) and X9.42 (Diffie-Hellman)
Header Encrypting Key
Data from Member's Profile:
Domain Name and Value
Header Encrypting Key
Current Maintenance Level and Value
Public Keys Corresponding to Credentials Used
e3xDES
Encrypted Header
Domain Name
Ephemeral Diffie-Hellman Public Key
Credential 1 Index
Credential 2 Index
Generated Diffie-Hellman Key Pair
Credential n Index
n-th selected credential Public Key with Private Key
Second selected credential Public Key with Private Key
First selected credential PublicKey with Private Key
Private key
Plaintext Header
hSHA1
Encrypted Random Value
e3xDES
System Generated Random Value
Domain Value and Name from Credentials
Current Maintenance Level
Current Maintenance Value
c
Working Key
Legend
e3xDES Triple DES encryption
hSHA1 SHA1 hash function
c CKM combiner function

FIG. 6

Decryption using X9.69 (CKM), X9.52 (3xDES) and X9.42 (Diffie-Hellman)

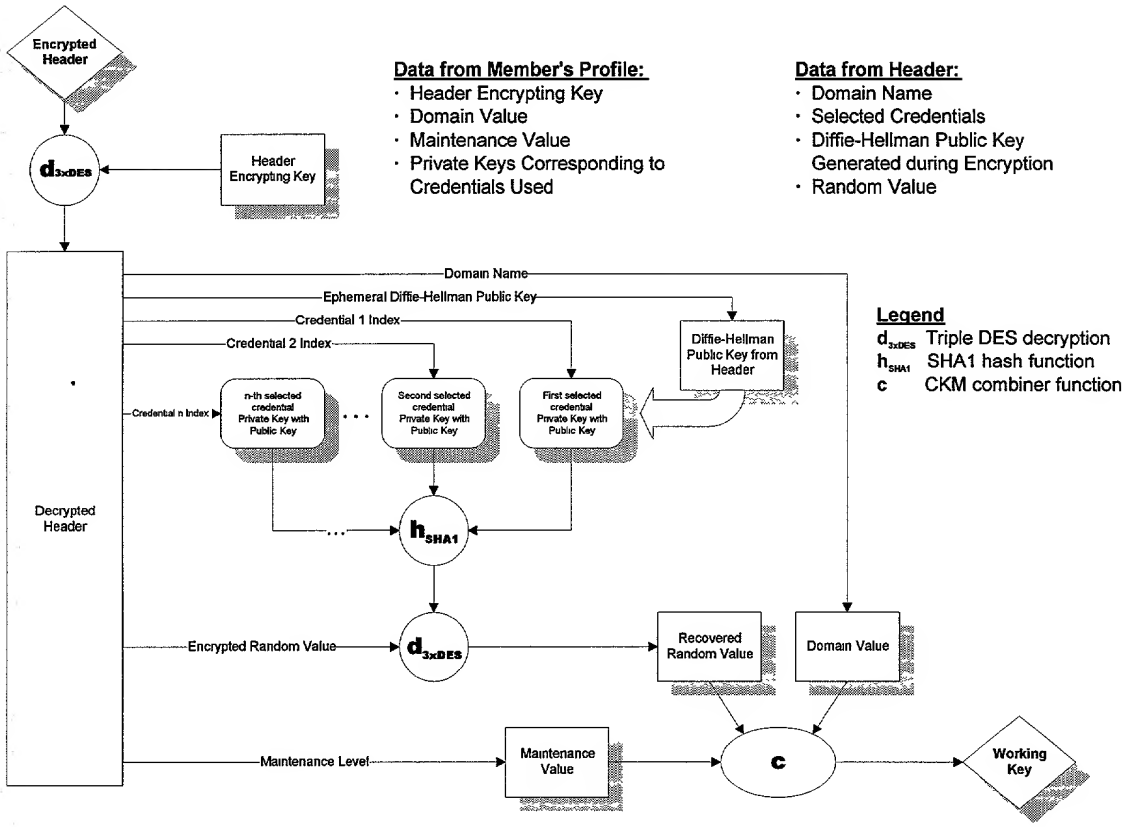


FIG. 7

Encryption using X9.69 (CKM), X9.52 (3xDES) and RSA

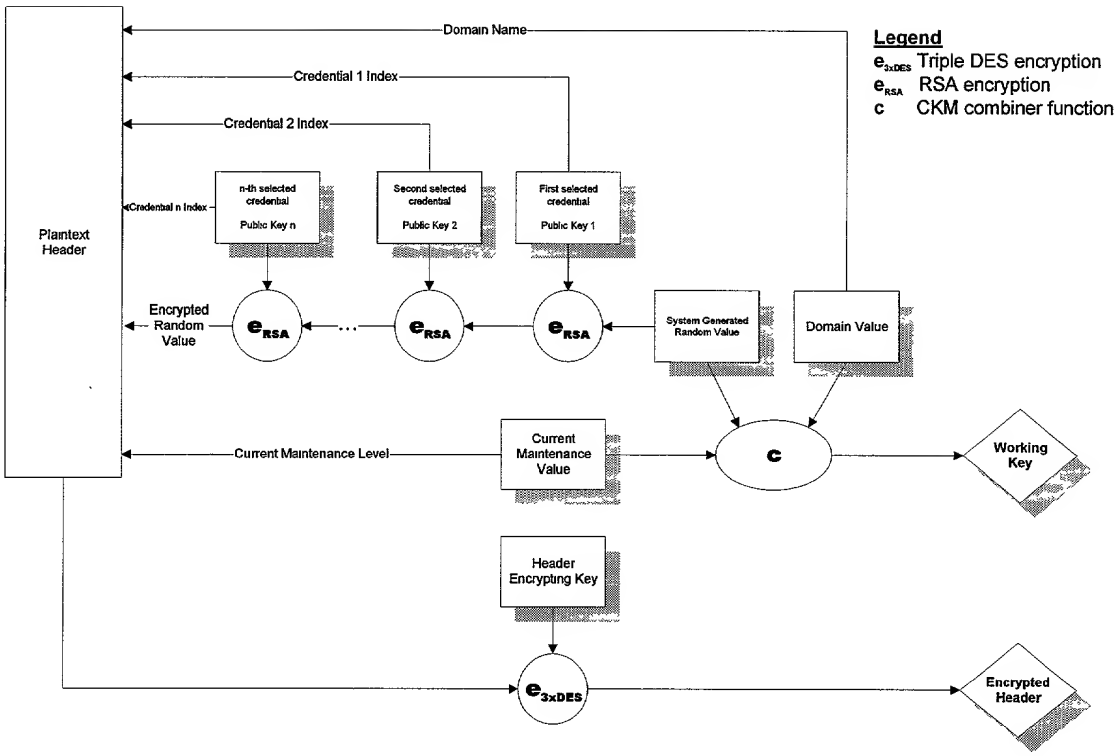


FIG. 8

Decryption using X9.69 (CKM), X9.52 (3xDES) and RSA

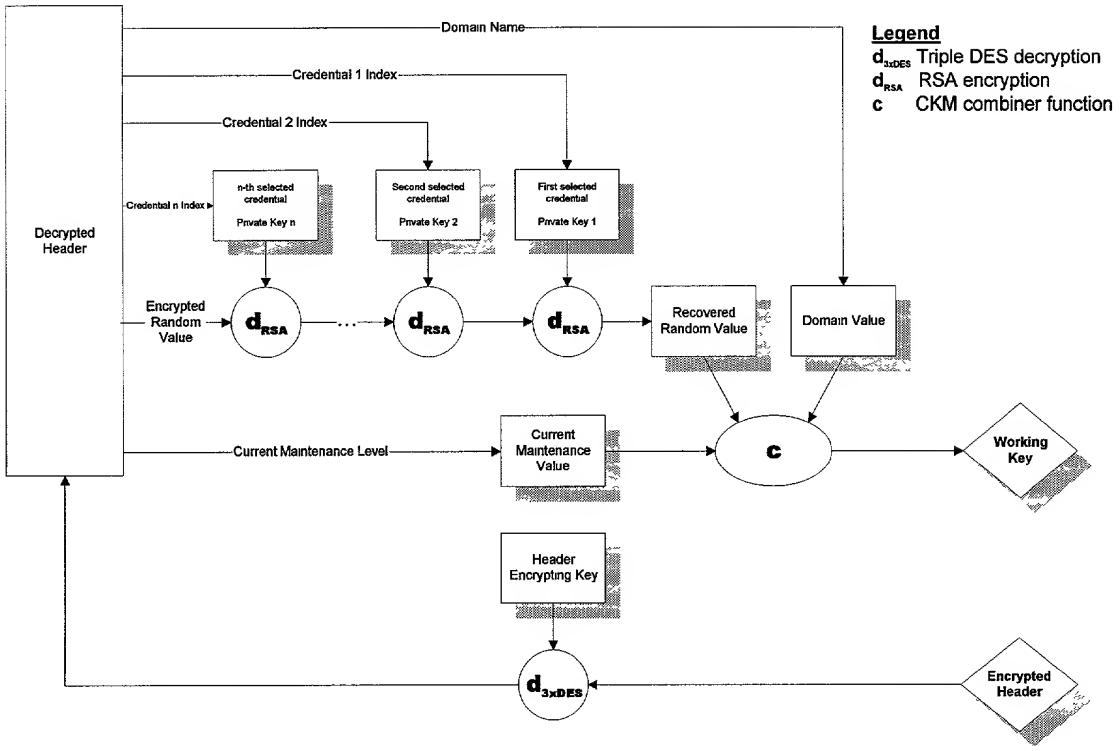


FIG. 9

PCT/US2003/040363

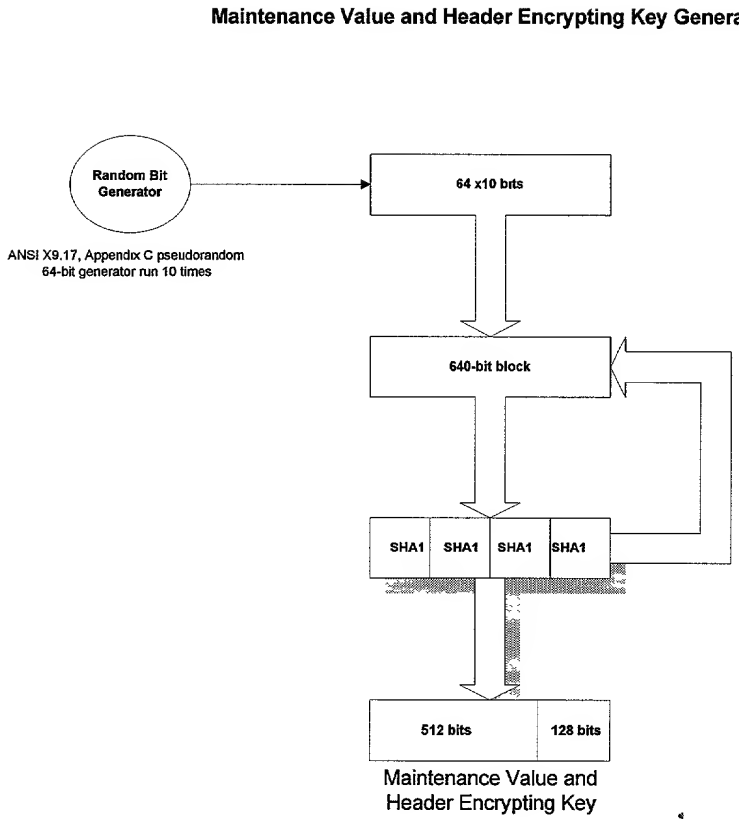


FIG. 10

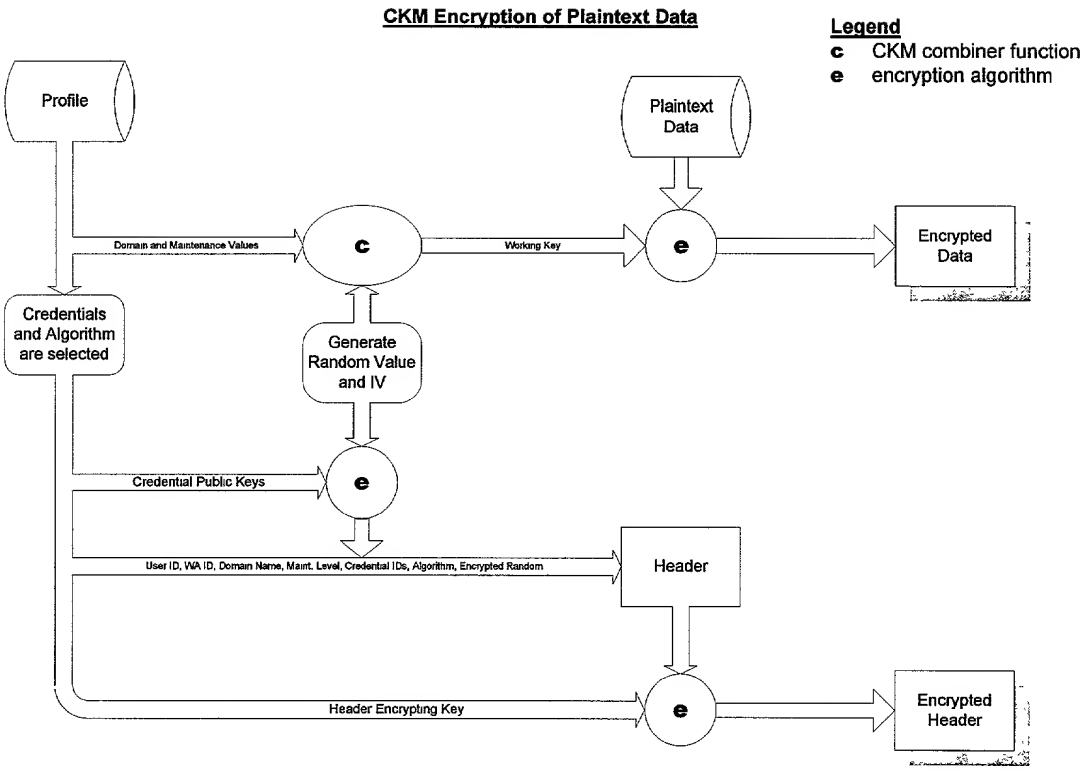

CKM Encryption of Plaintext Data
Legend
c CKM combiner function
e encryption algorithm
Profile
Plaintext Data
Domain and Maintenance Values
c
Working Key
e
Encrypted Data
Credentials and Algorithm are selected
Generate Random Value and IV
Credential Public Keys
e
User ID, WA ID, Domain Name, Maint. Level, Credential IDs, Algorithm, Encrypted Random
Header
Header Encrypting Key
e
Encrypted Header

FIG. 11

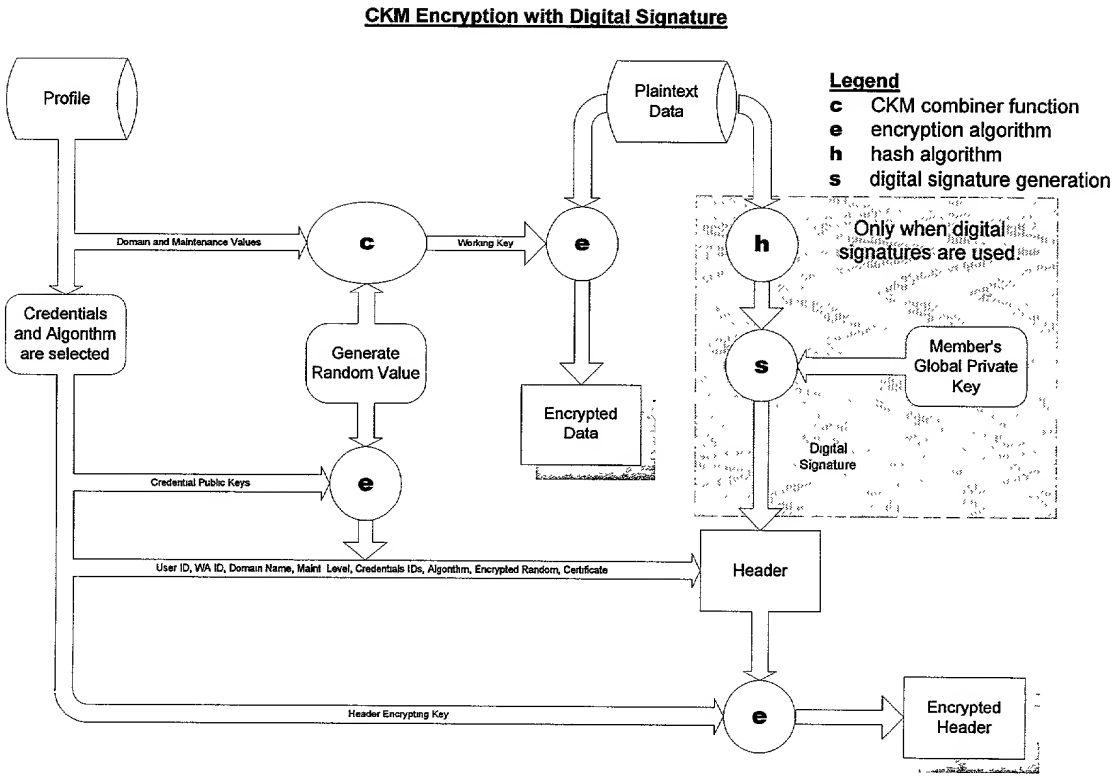

CKM Encryption with Digital Signature
Profile
Plaintext Data
Legend
c CKM combiner function
e encryption algorithm
h hash algorithm
s digital signature generation
Domain and Maintenance Values
c
Working Key
e
h
Only when digital signatures are used:
Credentials and Algorithm are selected
Generate Random Value
Encrypted Data
s
Member's Global Private Key
Digital Signature
Credential Public Keys
e
User ID, WA ID, Domain Name, Maint Level, Credentials IDs, Algorithm, Encrypted Random, Certificate
Header
Header Encrypting Key
e
Encrypted Header

FIG. 12

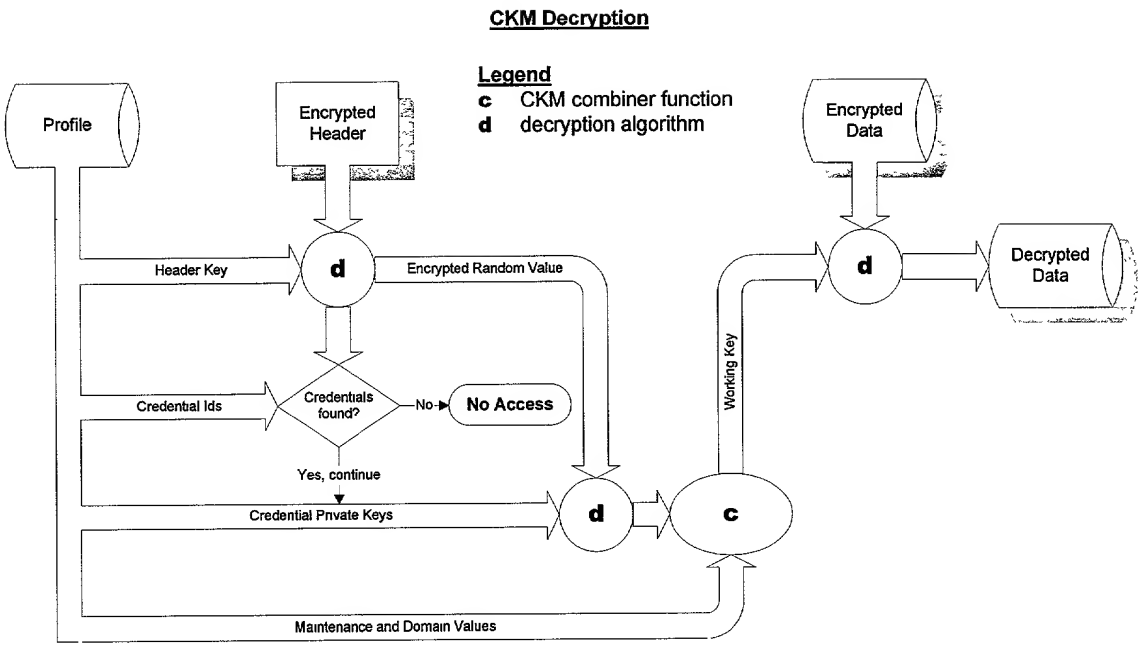

CKM Decryption
Legend
c CKM combiner function
d decryption algorithm
Profile
Encrypted Header
Encrypted Data
Header Key
d
Encrypted Random Value
d
Decrypted Data
Credential Ids
Credentials found?
No
No Access
Working Key
Yes, continue
Credential Private Keys
d
c
Maintenance and Domain Values

FIG. 13

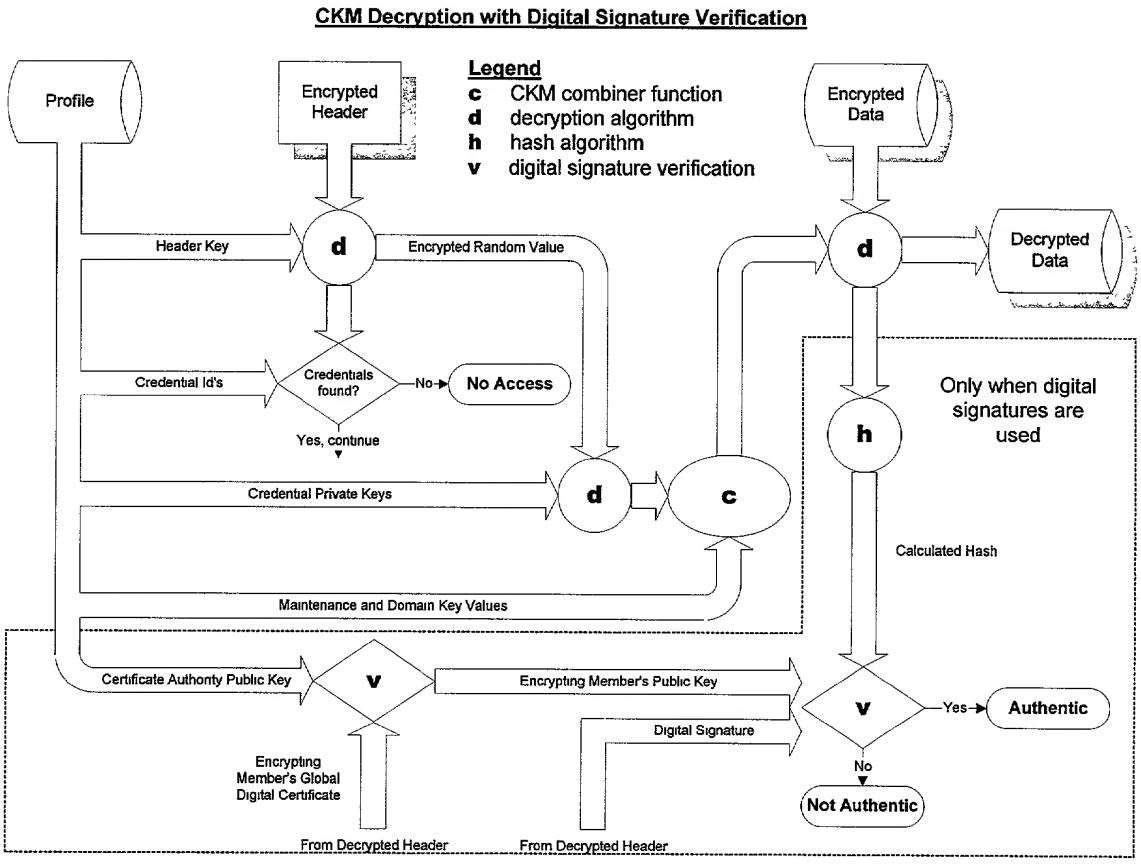

CKM Decryption with Digital Signature Verification
Legend
c CKM combiner function
d decryption algorithm
h hash algorithm
v digital signature verification
Profile
Encrypted Header
Encrypted Data
Header Key
d
Encrypted Random Value
Decrypted Data
Credential Id's
Credentials found?
No
No Access
Yes, continue
Only when digital signatures are used
h
Credential Private Keys
d
c
Calculated Hash
Maintenance and Domain Key Values
Certificate Authority Public Key
v
Encrypting Member's Public Key
v
Yes
Authentic
Digital Signature
Encrypting Member's Global Digital Certificate
No
Not Authentic
From Decrypted Header
From Decrypted Header

FIG. 14

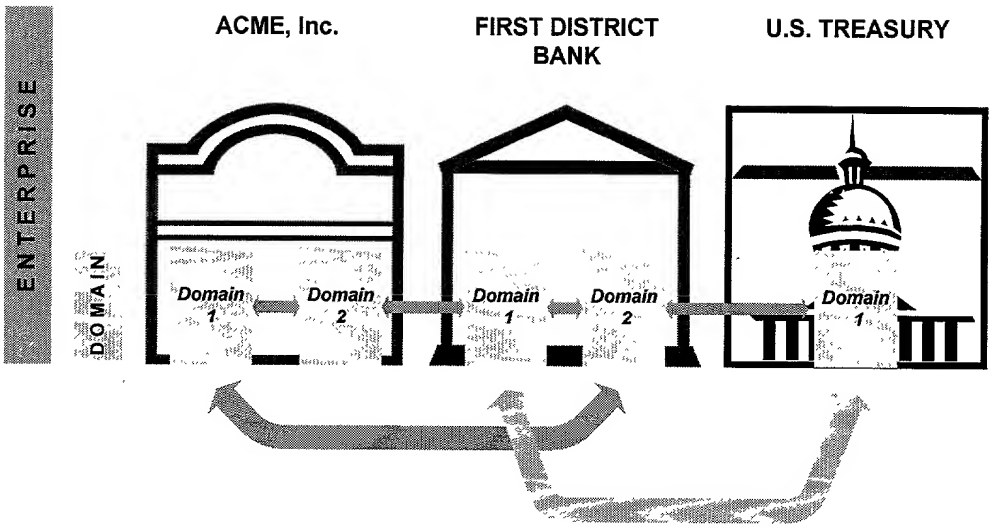

ENTERPRISE
DOMAIN
ACME, Inc.
FIRST DISTRICT BANK
U.S. TREASURY
Domain 1
Domain 2
Domain 1
Domain 2
Domain 1

FIG. 15

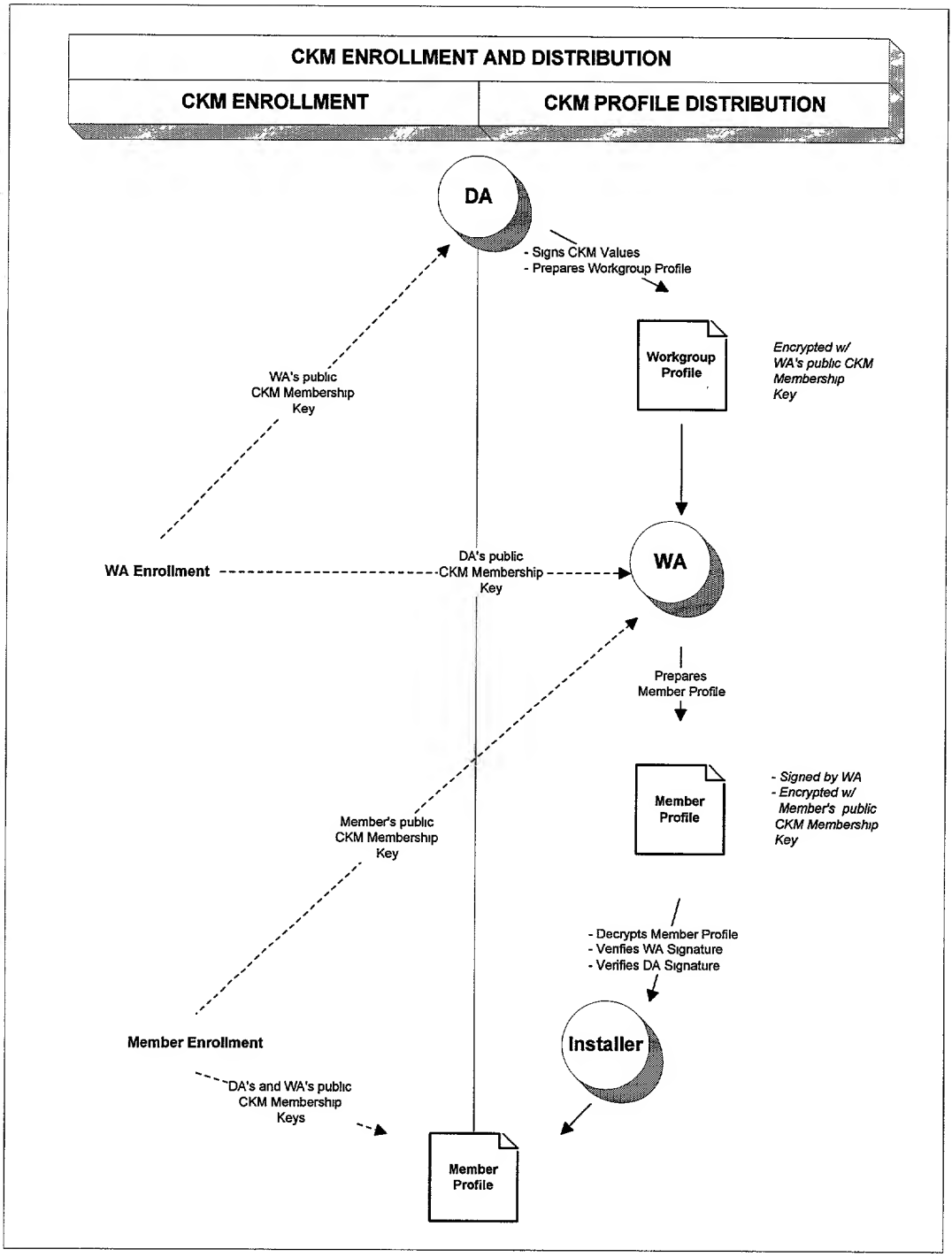

CKM ENROLLMENT AND DISTRIBUTION
CKM ENROLLMENT
CKM PROFILE DISTRIBUTION
DA
- Signs CKM Values
- Prepares Workgroup Profile
Workgroup Profile
Encrypted w/ WA's public CKM Membership Key
WA's public CKM Membership Key
WA Enrollment
DA's public CKM Membership Key
WA
Prepares Member Profile
Member Profile
- Signed by WA
- Encrypted w/ Member's public CKM Membership Key
Member's public CKM Membership Key
- Decrypts Member Profile
- Verifies WA Signature
- Verifies DA Signature
Installer
Member Enrollment
DA's and WA's public CKM Membership Keys
Member Profile

FIG. 16

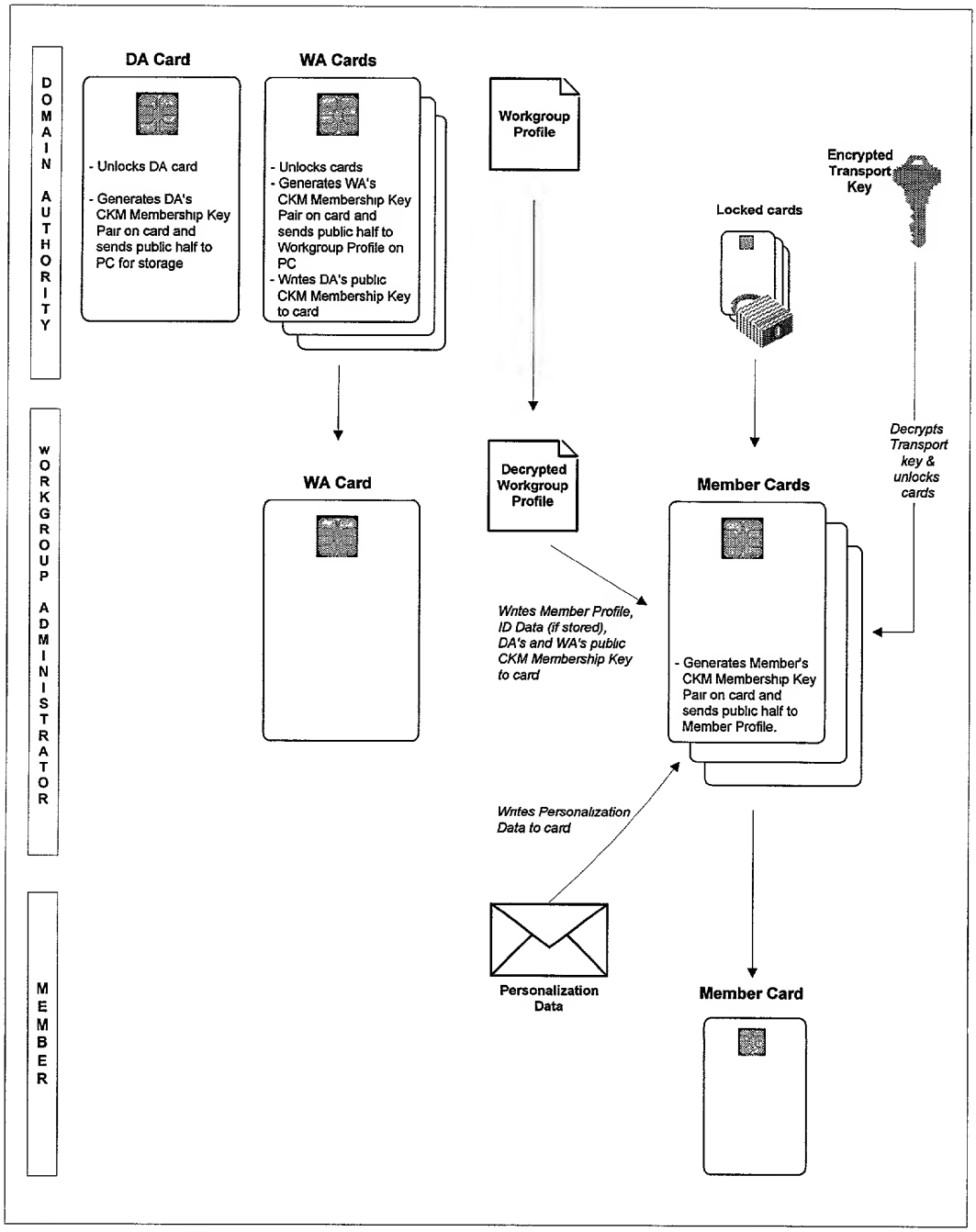

DOMAIN AUTHORITY
WORKGROUP ADMINISTRATOR
MEMBER
DA Card
- Unlocks DA card
- Generates DA's CKM Membership Key Pair on card and sends public half to PC for storage
WA Cards
- Unlocks cards
- Generates WA's CKM Membership Key Pair on card and sends public half to Workgroup Profile on PC
- Writes DA's public CKM Membership Key to card
Workgroup Profile
Encrypted Transport Key
Locked cards
Decrypts Transport key & unlocks cards
WA Card
Decrypted Workgroup Profile
Member Cards
Writes Member Profile, ID Data (if stored), DA's and WA's public CKM Membership Key to card
- Generates Member's CKM Membership Key Pair on card and sends public half to Member Profile.
Writes Personalization Data to card
Personalization Data
Member Card

FIG. 17

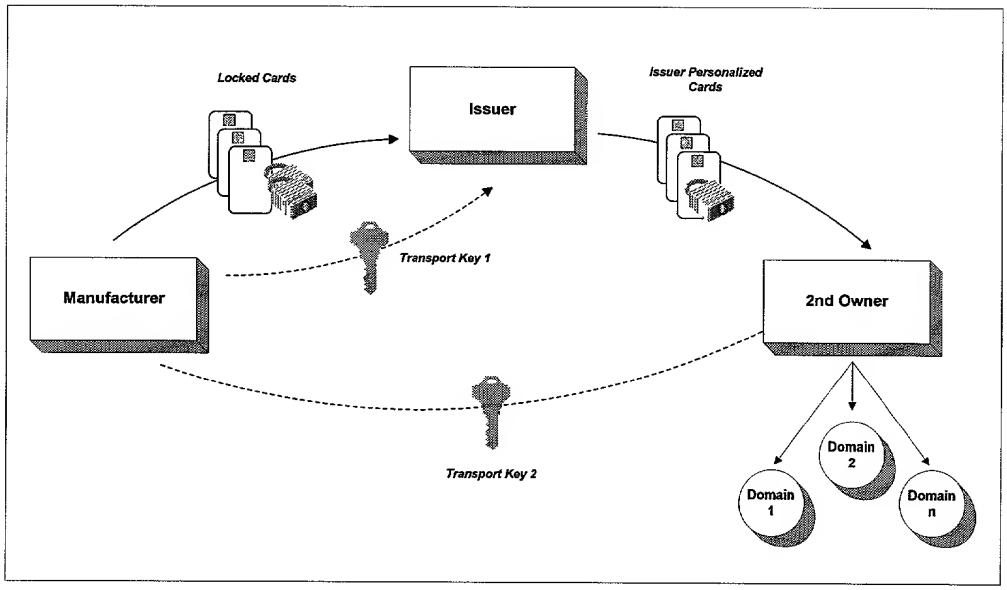

Locked Cards
Issuer
Issuer Personalized Cards
Transport Key 1
Manufacturer
2nd Owner
Transport Key 2
Domain 1
Domain 2
Domain n

FIG. 18

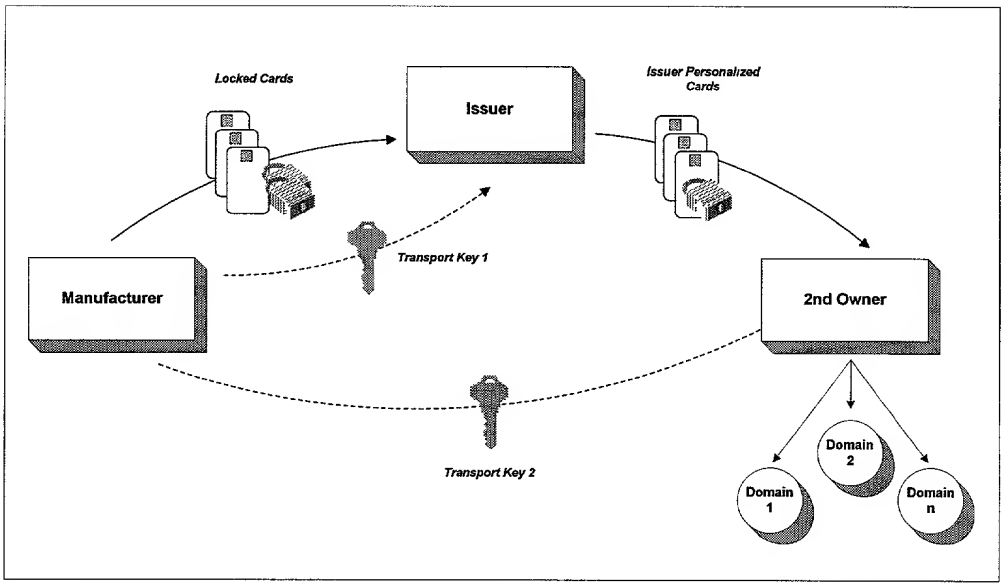

Locked Cards
Issuer
Issuer Personalized Cards
Transport Key 1
Manufacturer
2nd Owner
Transport Key 2
Domain 1
Domain 2
Domain n

FIG. 19

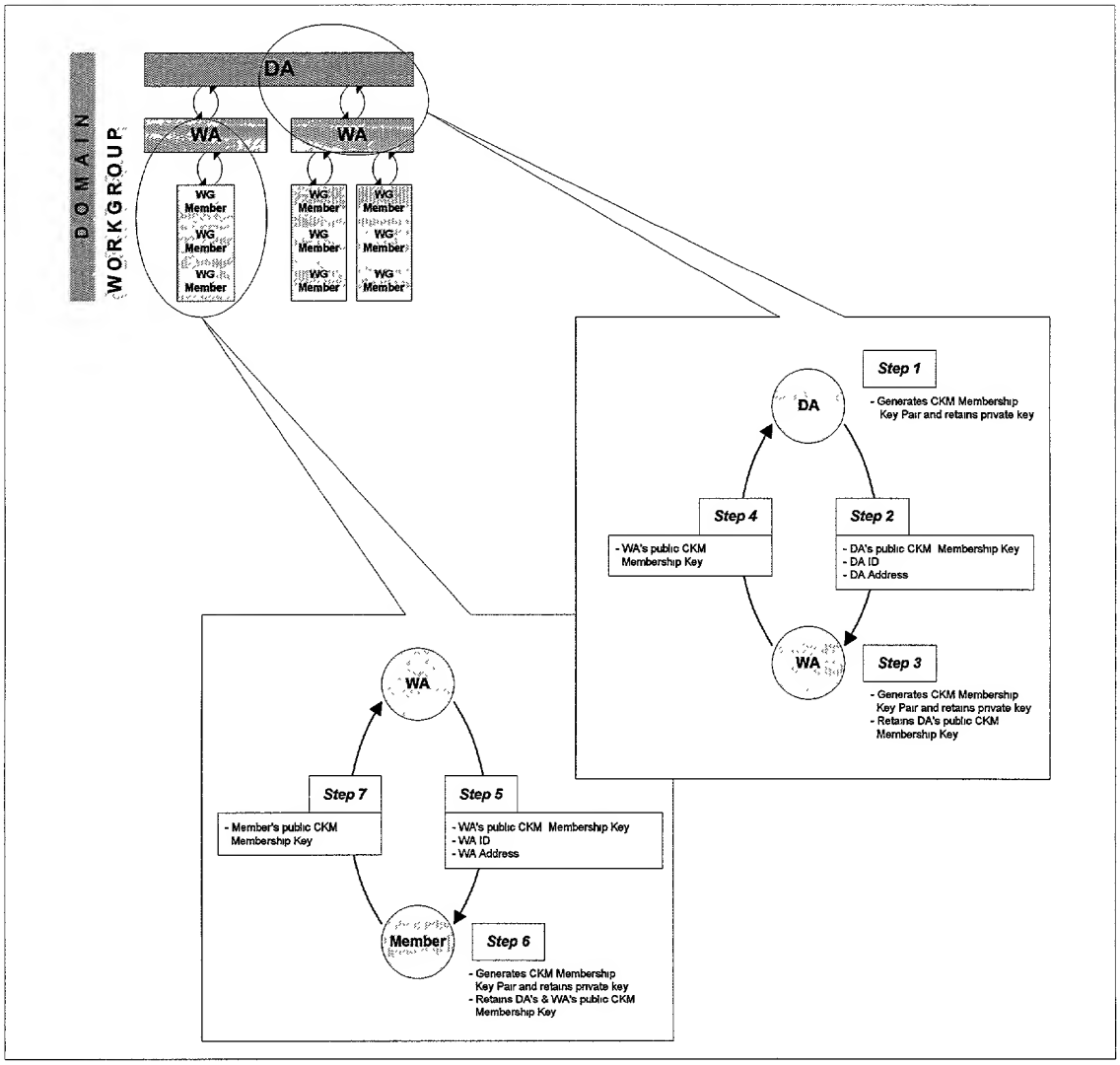

DOMAIN
WORKGROUP
DA
WA
WA
WG Member
WG Member
WG Member
WG Member
WG Member
WG Member
WG Member
WG Member
Step 1
- Generates CKM Membership Key Pair and retains private key
DA
Step 4
- WA's public CKM Membership Key
Step 2
- DA's public CKM Membership Key
- DA ID
- DA Address
WA
Step 3
- Generates CKM Membership Key Pair and retains private key
- Retains DA's public CKM Membership Key
WA
Step 7
- Member's public CKM Membership Key
Step 5
- WA's public CKM Membership Key
- WA ID
- WA Address
Member
Step 6
- Generates CKM Membership Key Pair and retains private key
- Retains DA's & WA's public CKM Membership Key

FIG. 20

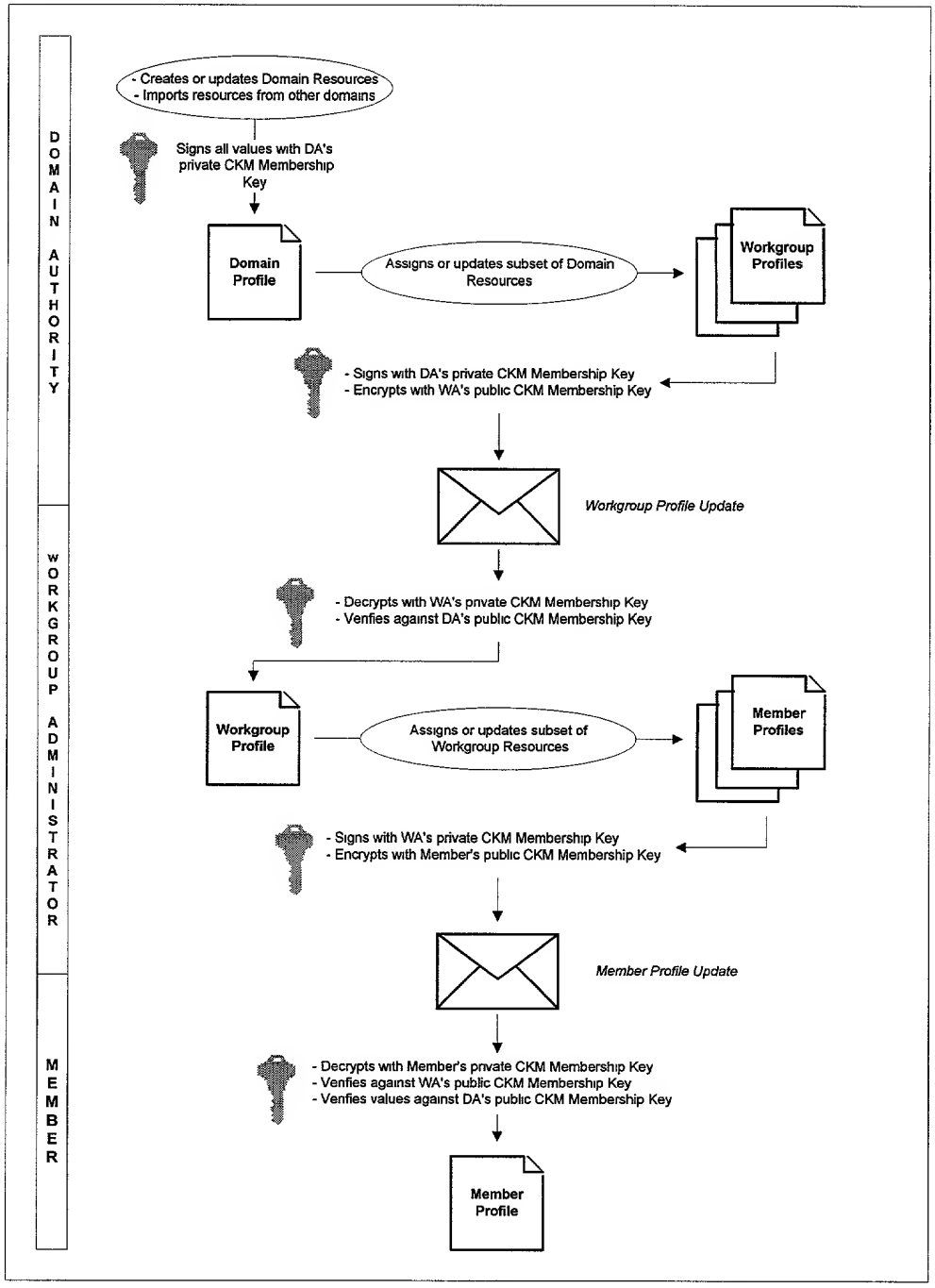

DOMAIN AUTHORITY
WORKGROUP ADMINISTRATOR
MEMBER
- Creates or updates Domain Resources
- Imports resources from other domains
Signs all values with DA's private CKM Membership Key
Domain Profile
Assigns or updates subset of Domain Resources
Workgroup Profiles
- Signs with DA's private CKM Membership Key
- Encrypts with WA's public CKM Membership Key
Workgroup Profile Update
- Decrypts with WA's private CKM Membership Key
- Verifies against DA's public CKM Membership Key
Workgroup Profile
Assigns or updates subset of Workgroup Resources
Member Profiles
- Signs with WA's private CKM Membership Key
- Encrypts with Member's public CKM Membership Key
Member Profile Update
- Decrypts with Member's private CKM Membership Key
- Verifies against WA's public CKM Membership Key
- Verifies values against DA's public CKM Membership Key
Member Profile

FIG. 21

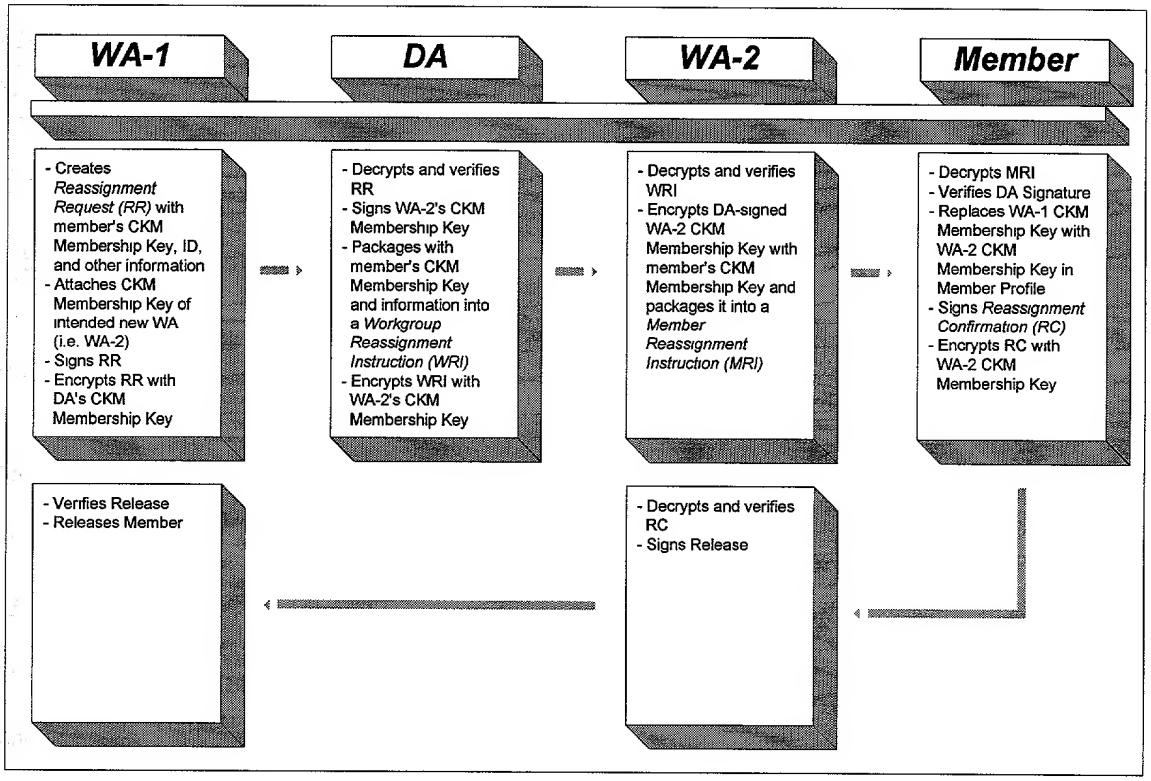

WA-1
DA
WA-2
Member
- Creates *Reassignment Request (RR)* with member's CKM Membership Key, ID, and other information
- Attaches CKM Membership Key of intended new WA (i.e. WA-2)
- Signs RR
- Encrypts RR with DA's CKM Membership Key
- Decrypts and verifies RR
- Signs WA-2's CKM Membership Key
- Packages with member's CKM Membership Key and information into a *Workgroup Reassignment Instruction (WRI)*
- Encrypts WRI with WA-2's CKM Membership Key
- Decrypts and verifies WRI
- Encrypts DA-signed WA-2 CKM Membership Key with member's CKM Membership Key and packages it into a *Member Reassignment Instruction (MRI)*
- Decrypts MRI
- Verifies DA Signature
- Replaces WA-1 CKM Membership Key with WA-2 CKM Membership Key in Member Profile
- Signs *Reassignment Confirmation (RC)*
- Encrypts RC with WA-2 CKM Membership Key
- Verifies Release
- Releases Member
- Decrypts and verifies RC
- Signs Release

FIG. 22

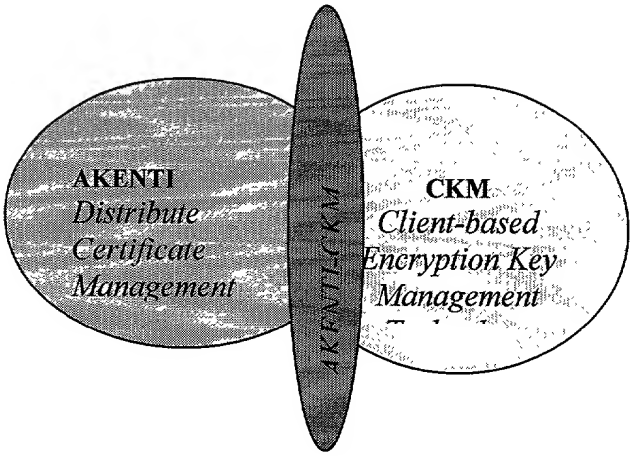
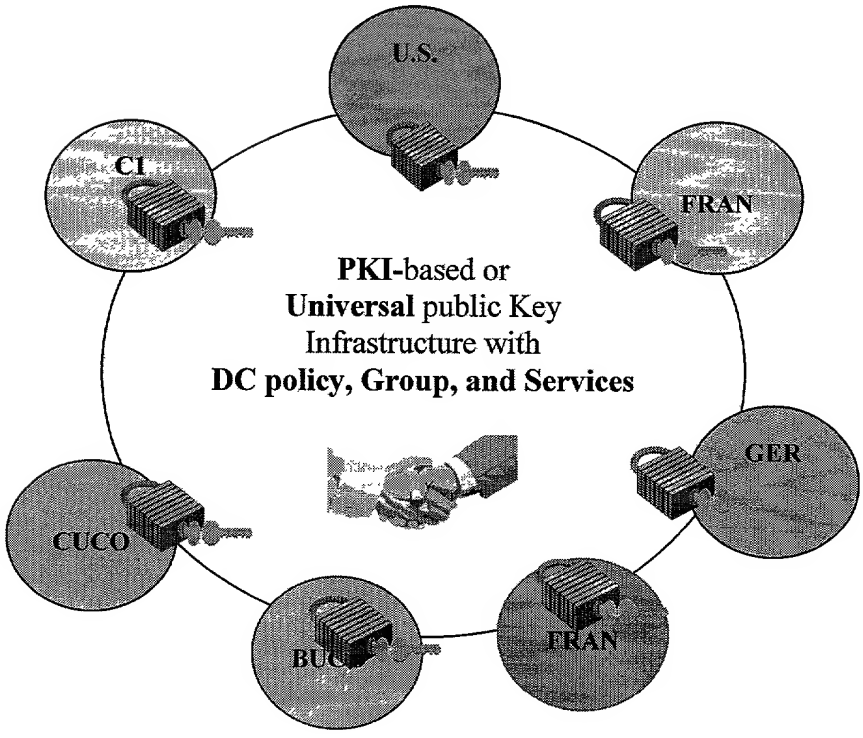

AKENTI
Distribute
Certificate
Management
AKENTI-CKM
CKM
Client-based
Encryption Key
Management

FIG. 23

ACKMENTI


U.S.
CI
FRAN
PKI-based or
Universal public Key
Infrastructure with
DC policy, Group, and Services
GER
CUCO
BUC
FRAN

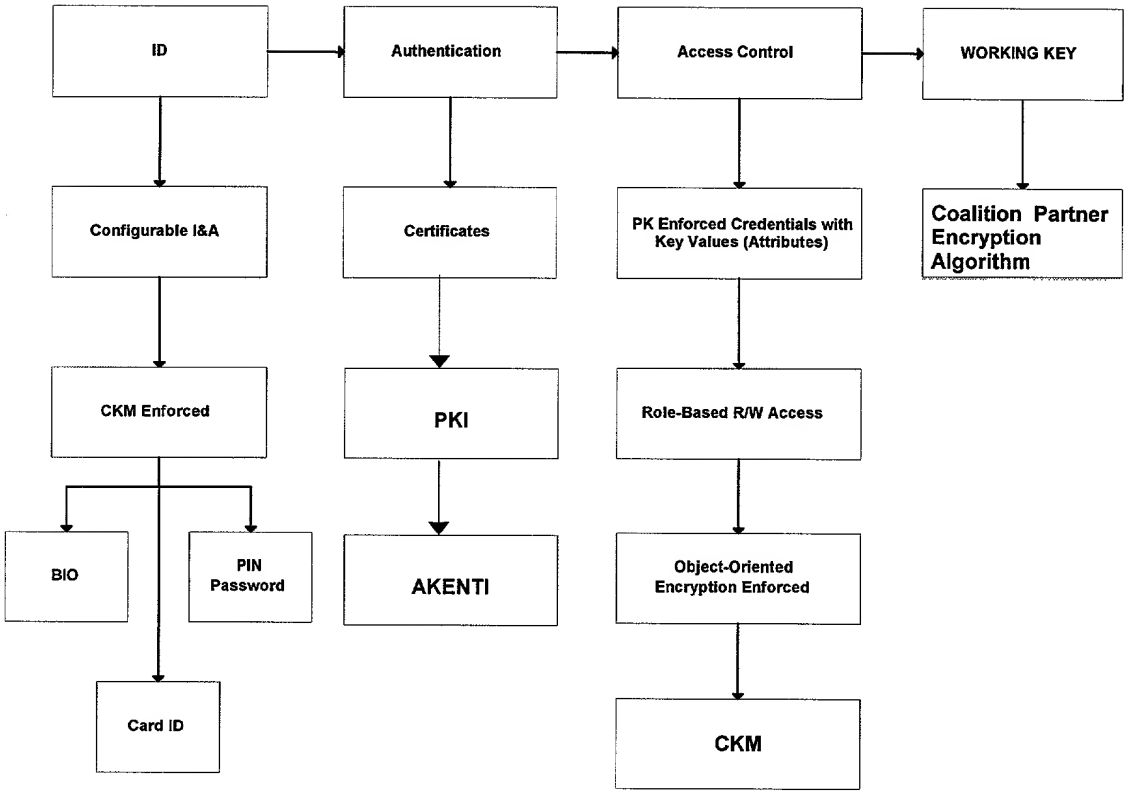

ID
Authentication
Access Control
WORKING KEY
Configurable I&A
Certificates
PK Enforced Credentials with Key Values (Attributes)
Coalition Partner Encryption Algorithm
CKM Enforced
PKI
Role-Based R/W Access
BIO
PIN Password
AKENTI
Object-Oriented Encryption Enforced
Card ID
CKM

FIG. 24

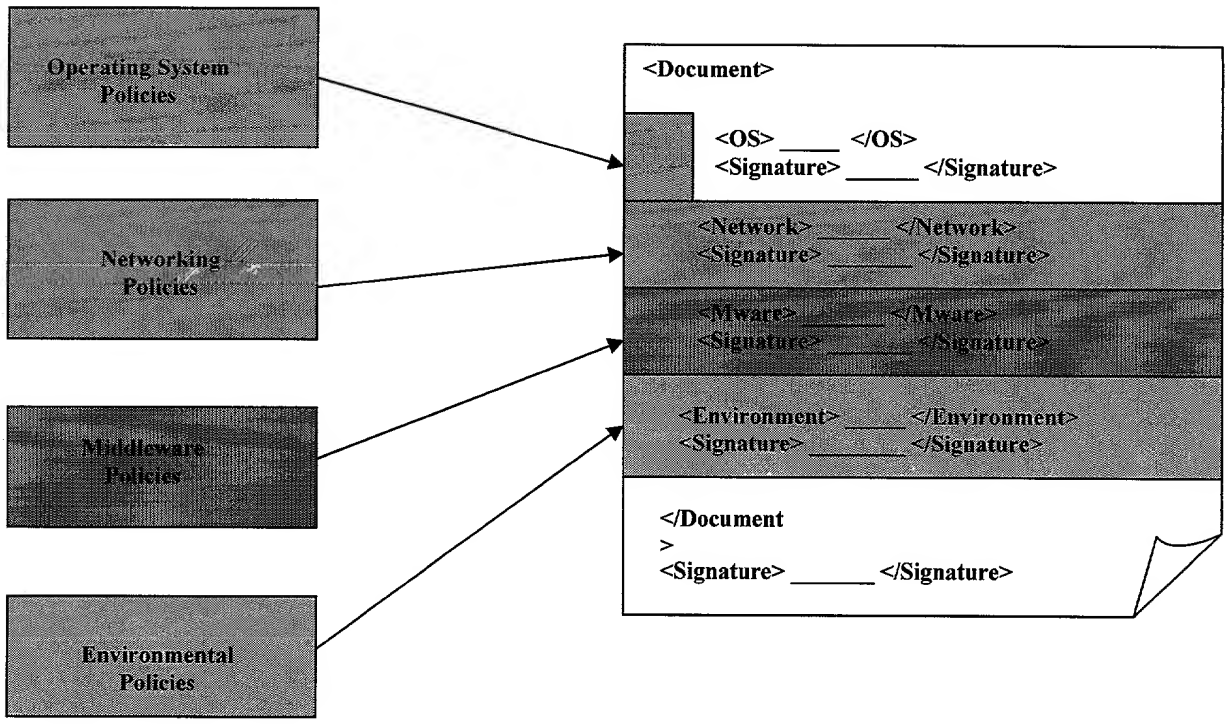

Operating System Policies
Networking Policies
Middleware Policies
Environmental Policies
<Document>
<OS> ____ </OS>
<Signature> _____ </Signature>
<Network> _____ </Network>
<Signature> _____ </Signature>
<Mware> _____ </Mware>
<Signature> _____ </Signature>
<Environment> ____ </Environment>
<Signature> _____ </Signature>
</Document
>
<Signature> _____ </Signature>

FIG. 25

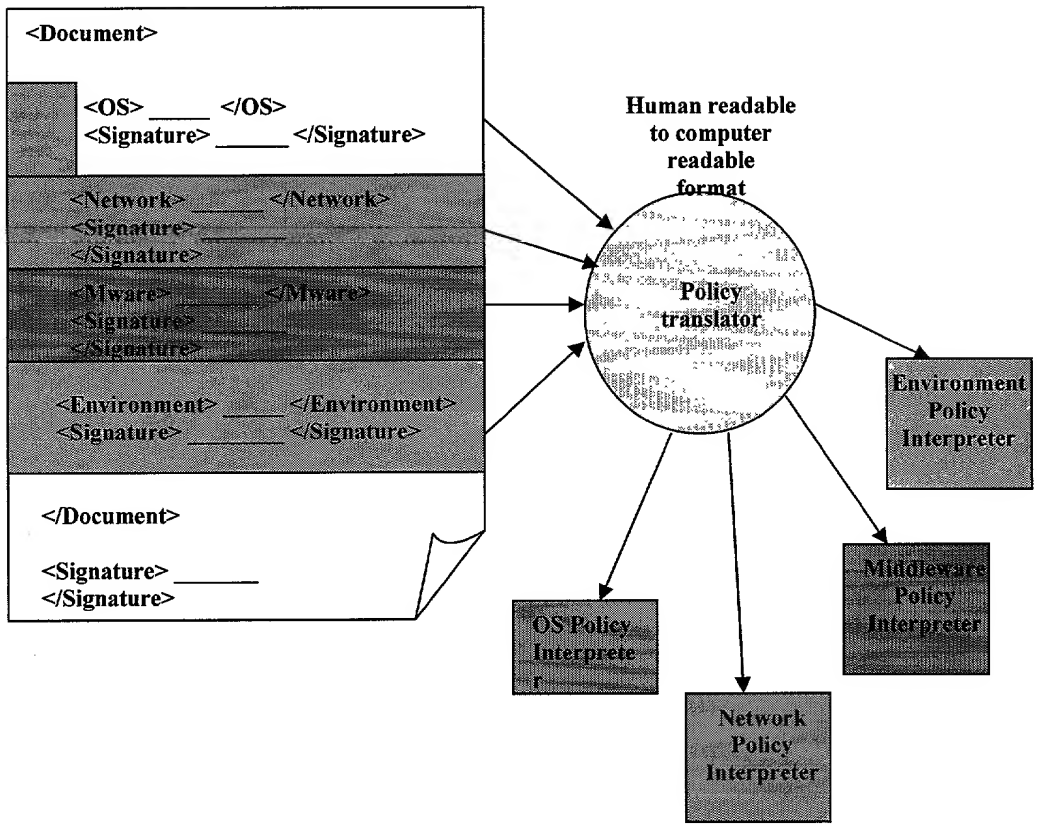
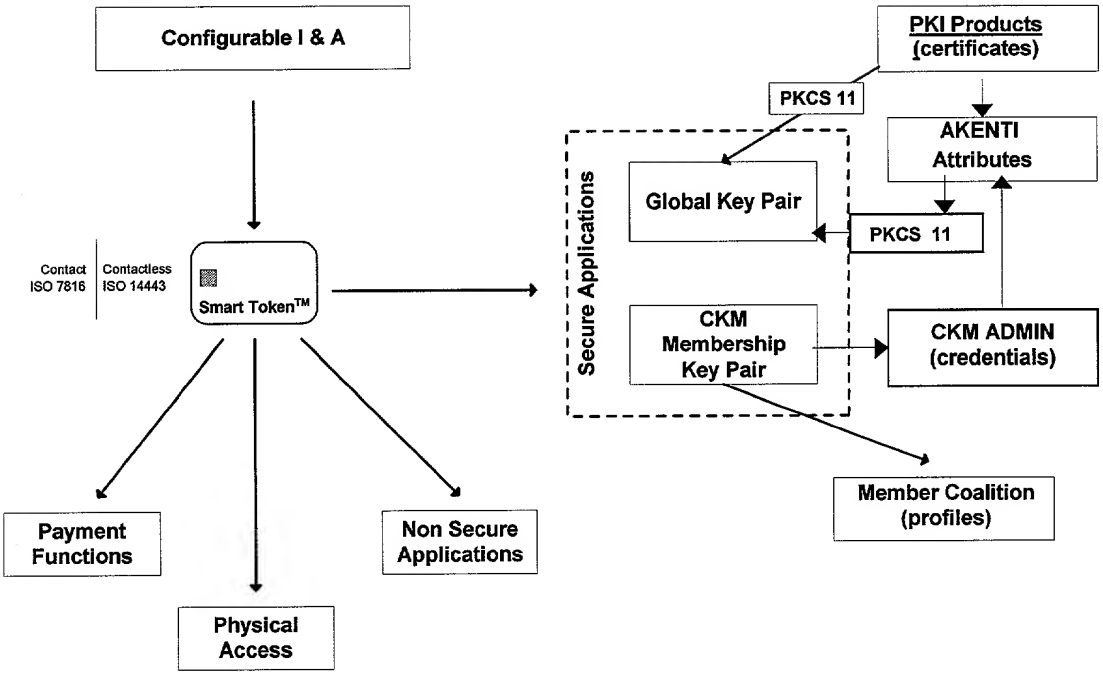

<Document>
<OS> _____ </OS>
<Signature> _____ </Signature>
<Network> _____ </Network>
<Signature> _____
</Signature>
<Mware> _____ </Mware>
<Signature>
</Signature>
<Environment> _____ </Environment>
<Signature> _____ </Signature>
</Document>
<Signature> _____
</Signature>
Human readable to computer readable format
Policy translator
Environment Policy Interpreter
Middleware Policy Interpreter
Network Policy Interpreter
OS Policy Interpreter

FIG. 26



CKM™	Constructive Key Management
I&A	Identification and Authentication
PK	Public Key
PKI	Public Key Infrastructure

FIG. 27

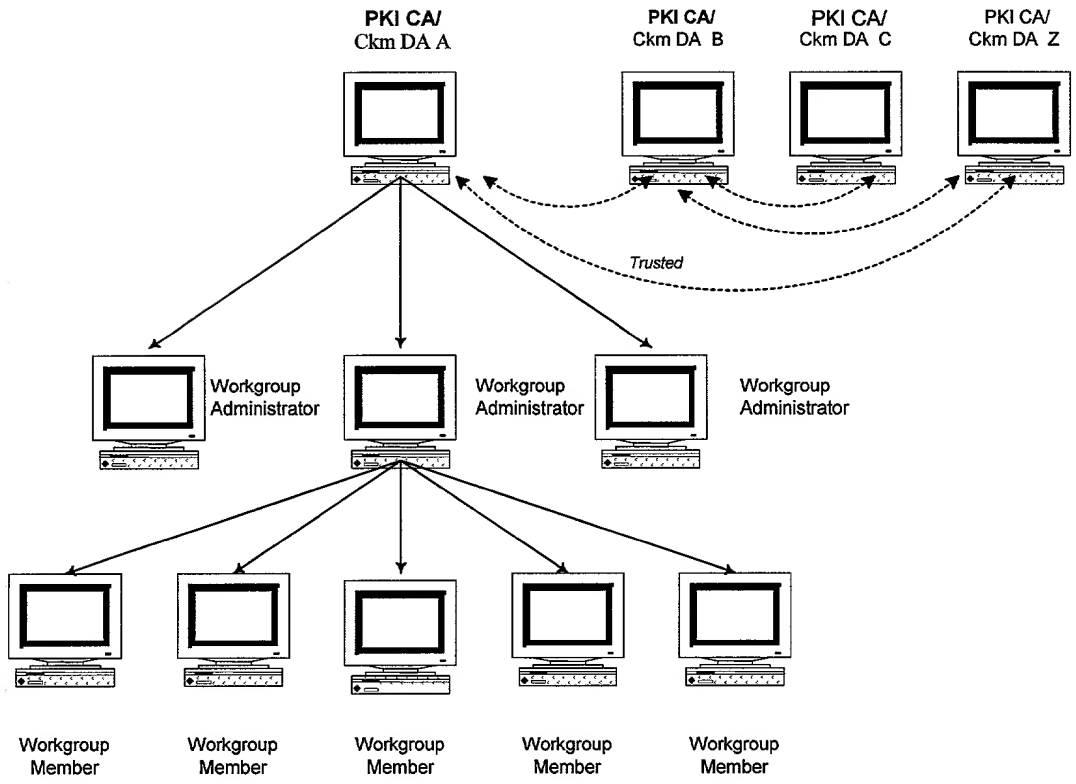

PKI CA/
Ckm DA A
PKI CA/
Ckm DA B
PKI CA/
Ckm DA C
PKI CA/
Ckm DA Z
Trusted
Workgroup
Administrator
Workgroup
Administrator
Workgroup
Administrator
Workgroup
Member
Workgroup
Member
Workgroup
Member
Workgroup
Member
Workgroup
Member

FIG. 28